(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 April 2004 (08.04.2004)

PCT

(10) International Publication Number
WO 2004/030312 A1

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number:
PCT/IB2003/004123

(22) International Filing Date:
22 September 2003 (22.09.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/414,944 30 September 2002 (30.09.2002) US
60/445,263 5 February 2003 (05.02.2003) US

(71) Applicant *(for all designated States except US)*: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: EPSTEIN, Michael, A. [US/US]; P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US). GRUMIAUX, Frederic [US/US]; P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US).

(74) Common Representative: KONINKLIJKE PHILIPS ELECTRONICS N.V.; Intellectual Property & Standards, c/o THORNE, Gregory, L., P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

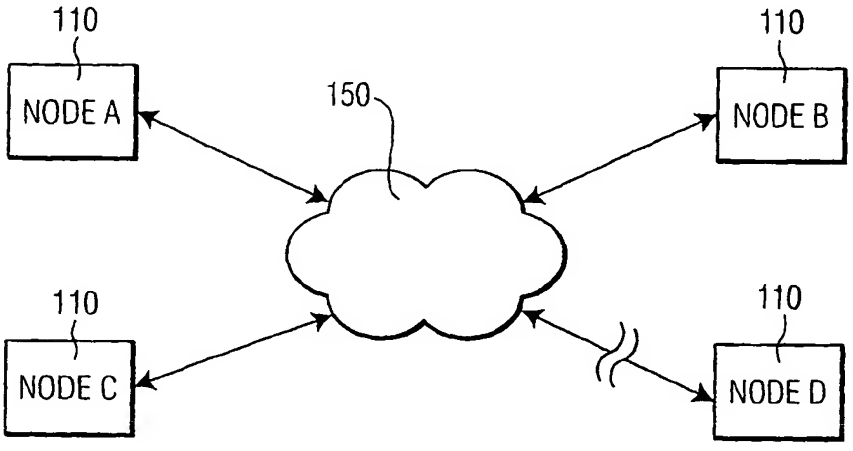
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO*

[Continued on next page]

(54) Title: VERIFYING A NODE ON A NETWORK



(57) Abstract: A system and method includes timing parameters within a node-verification protocol, such as OCPS, to facilitate a determination of the proximity of a target node to a source node. The node-verification protocol includes a query-response sequence, between the source node and the target node. The source node establishes a lower bound on the distance between the source node and the target node based on a measure of the time required to effect this query-response sequence including the time required to communicate the query and response, as well as the time required to process the query and generate the response. The target node includes a measure of the time required to process the query and generate the response to the source node. The source node subtracts this time from the total query-response time to determine the time consumed for the communication.

WO 2004/030312 A1

patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

VERIFYING A NODE ON A NETWORK

This invention relates to the field of communications security, and in particular, to a system and method that verifies the proximity of a node on a network.

Network security can often be enhanced by distinguishing between 'local' nodes and 'remote' nodes on the network. Local nodes, for example, are typically located within a particular physical environment, and it can be assumed that users within this physical environment are authorized to access the network. Remote nodes, on the other hand, are susceptible to unauthorized physical access. Additionally, unauthorized intruders on a network typically access the network remotely, via telephone or other communication channels. Because of the susceptibility of the network to unauthorized access via remote nodes, network security can be enhanced by imposing stringent security measures, or access restrictions, on remote nodes, while not encumbering local nodes with this same restrictions.

It is an object of this invention to provide a system and method that facilitates a determination of whether a node on a network is local or remote. It is a further object of this invention to provide a system and method that facilitates a secure determination of whether a node on a network is local or remote. It is a further object of this invention to integrate this determination with a system or method that verifies the authenticity of the node on the network.

These objects and others are achieved by a system and method that includes timing parameters within a node-verification protocol, such as the Open Copy Protection System (OCPS), to facilitate a determination of the proximity of a target node to a source node. The node-verification protocol includes a query-response sequence, wherein the source node communicates a query to the target node, and the target node communicates a corresponding response to the source node. The source node establishes a lower bound on the distance between the source node and the target node, based on a measure of the time required to effect this query-response sequence. The time required to effect this sequence includes the time required to communicate the query and response, as well as the time required to process the query and generate the response. The target node includes a measure of the time required to process the query and generate the response to the source node. The source node subtracts this time from the total query-response time to determine

the time consumed for the communication. This communication time is compared to a threshold value to determine whether the target node is local or remote relative to the source node.

FIG. 1 illustrates an example block diagram of a network of nodes.

FIG. 2 illustrates an example block diagram of a source and target node that effect a query-response protocol in accordance with this invention.

Throughout the drawings, the same reference numeral refers to the same element, or an element that performs substantially the same function.

FIG. 1 illustrates an example block diagram of a network 150 of nodes 110. One of the nodes, NodeD 110, is illustrated as being distant from the other nodes 110. In accordance with this invention, each of the nodes 110 is configured to be able to determine the proximity of each other node 110. In a typical embodiment of this invention, the proximity determination is limited to a determination of whether the other node is "local" or "remote", although a more detailed determination of distances can be effected using the techniques disclosed herein.

FIG. 2 illustrates an example block diagram of a source node 110S and target node 110T that effect a query-response protocol to determine the proximity of the target node 110T to the source node 110S in accordance with this invention. The source node 110S includes a processor 210 that initiates a query, and a communications device 220 that transmits the query to the target node 110T. The target node 110T receives the query and returns a corresponding response, via its communications device 230. To assure that the response corresponds to the communicated query, the protocol calls for the target node 110T to process at least a portion of the query and to include a result of this processing in the response, via a processor 240.

The source node 110S is configured to measure the time consumed by the query-response process, illustrated in FIG. 2 as $T_{query\text{-}response}$ 280. This query-response time 280 includes the time to communicate the query and response, $T_{communicate}$ 260, as well as the time to process the query and generate the response at the target node 110T, $T_{process}$ 270. In accordance with this invention, the target node 110T is configured to include a measure of this processing time 270 within the response provided to the source node 110S. The source node 110S subtracts the processing time 270 from the query-response time 280 to determine the communication time 260. Using known techniques, the distance between the

source 110S and target 110T can be calculated using this determined communication time 260. As noted above, in a typical embodiment, the communication time 260 is used to determine whether the target 110T is local or remote from the source 110S. This determination is made in a preferred embodiment of this invention by comparing the communication time 260 to a nominal threshold value, typically not more than a few milliseconds. If the communication time 260 is below the threshold, the target 110T is determined to be local; otherwise, it is determined to be remote.

In a typical embodiment, the source 110S uses the remote/local proximity determination to control subsequent communications with the target 110T. For example, some files may be permitted to be transferred only to local nodes, all communications with a remote node may be required to be encrypted, and so on. Optionally, multiple threshold levels may be defined to distinguish different ranges of distances, such as whether a remote target node is located within the same country as the source node, and so on.

Note that an unauthorized node can subvert the above process by providing a false processing time. In a preferred embodiment of this invention, the above query-response process is integrated within a node-authentication process, such as a key-exchange process, which typically includes one or more query-response sequences. By integrating the query-response process within the node-authentication process, the reported processing time is verified as being authentic.

The OCPS protocol, for example, includes an authentication stage, a key exchange stage, a key generation phase, and subsequent data transmission phases. The key exchange phase is effected via a modified Needham-Schroeder key exchange protocol, as described in "Handbook of Applied Cryptography", Menezes et al.

At the authentication stage, each of the source 110S and target 110T nodes authenticates a public key of each other.

At the start of the key exchange phase, the source 110S encrypts a random number and a random key, using the public key of the target 110T, and transmits both encryptions to the target 110T. In accordance with this invention, the source node 110S initiates a timer when these encryptions are transmitted to the target 110T.

The target 110T decrypts the random number and random key, using the private key of the target. The target 110T generates a new random number and a new random key, and encrypts the new random number, the new random key, and the decrypted random

number from the source 110S, using the public key of the source 110S, to form a response that is to be communicated to the source 110S. The target 110T optionally signs the response, using the target's private key. In accordance with this invention, the target 110T also includes a measure of the time required to effect the decryption, encryption, and signing within the signed response. This processing time is optionally encrypted using the public key of the source. Because this decryption, encryption, and signing process generally consumes the same amount of time at a given target node, the target node is preferably configured to provide a predefined processing time as the measure of time to effect this processing. By signing the response, the target 110T binds the reported processing time to the other parameters in the current response, thereby precluding an unauthorized replacement of the encrypted processing time with an alternative time that is encrypted using the public key of the source 110S.

When the source node 110S receives the response, it terminates the aforementioned timer. The source node 110S verifies the signed message, using the public key of the target 110T, and decrypts the random numbers and random key from the response, using the private key of the source 110S. If the processing time within the response is encrypted, it is also decrypted at this time by the source 110S, using the private key of the source 110S. In accordance with this invention, the source 110S subtracts the processing time from the time duration measured by the timer between the transmission of the encrypted query from the source 110S and the reception of the encrypted response from the target 110T to determine the round-trip communication time between source 110S and target 110T.

To confirm the key exchange, the source 110S transmits the decrypted new random number back to the target 110T. Both the source 110S and target 110T control subsequent communications based upon receipt of the proper decrypted random numbers. In accordance with this invention, the source 110S also controls subsequent communications based upon the determined communication time.

If both nodes are verified, subsequent communications between the source 110S and target 110T encrypt the communications using a session key that is a combination of the random keys, the public keys, and a session index.

The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise various arrangements which, although not explicitly described or shown herein, embody the principles of the invention

and are thus within its spirit and scope. For example, in the above described OCPS protocol, the target node 110T may also be configured to determine the proximity of the source node 110S, by timing the process between the transmission of the encrypted response and the receipt of the decrypted random number from the source 110S. In this embodiment, the source 110S is configured to include a measure of the time required to process the encrypted response and transmit the decrypted random number in the last key exchange message that includes the decrypted random number, digitally signed by the source 110S. The target 110T subtracts this processing time from its measured time between transmission and receipt to determine the round-trip target-source-target communication time, and thus the proximity of the source 110S to the target 110T. These and other system configuration and optimization features will be evident to one of ordinary skill in the art in view of this disclosure, and are included within the scope of the following claims.

CLAIMS:

1. A method of determining proximity of a target node to a source node, comprising:

communicating a query from the source node to the target node,

communicating a response from the target node to the source node,

the response from the target node including a measure of processing time required to generate the response based on the query,

receiving the response at the source node,

determining a measure of query-response time between communicating the query and receiving the response, and

determining the proximity of the target node based on a communication time that depends upon a difference between the measure of query-response time and the measure of processing time.

2. The method of claim 1, wherein

the query and response correspond to at least a portion of a cryptographic key-exchange protocol.

3. The method of claim 2, wherein

the key-exchange protocol corresponds to a Needham-Schroeder key-exchange protocol.

4. The method of claim 1, wherein

the query and response correspond to at least a portion of an OCPS protocol.

5. The method of claim 1, wherein

the measure of processing time at the target node is predefined.

6. The method of claim 1, wherein

determining the proximity includes comparing the communication time to a threshold value that distinguishes between local and remote nodes.

7. The method of claim 1, further including

restricting communications with the target node based on the proximity.

8. The method of claim 1, wherein

the response is cryptographically signed by the target node.

9. A node on a network including:

a communication device that is configured to receive a query from a source node and to transmit a corresponding response to the source node,

a processor that is configured to process the query and produce therefrom the response,

wherein

the response includes a measure of processing time required to process the query and produce the response.

10. The node of claim 9, wherein

the processor is configured to process the query and produce the response as part of a cryptographic key-exchange protocol.

11. The node of claim 10, wherein

the key-exchange protocol corresponds to a Needham-Schroeder key-exchange protocol.

12. The node of claim 9, wherein

the query and response correspond to at least a portion of an OCPS protocol initiated by the source node.

13. The node of claim 9, wherein

the measure of processing time is predefined.

14. The node of claim 9, wherein

the processor is further configured to cryptographically sign the response.

15. A node on a network including:

a communication device that is configured to transmit a query to a target node and to receive a corresponding response from the target node,

the response from the target node including a measure of processing time required to generate the response at the target node, and

a processor that is configured to:

generate the query,

receive the response,

measure a query-response time between generating the query and receiving the response, and

determine a proximity of the target node relative to the node based on a communication time that is dependent upon a difference between the query-response time and the measure of processing time.

16. The node of claim 15, wherein

the processor is configured to generate the query and receive the response as part of a cryptographic key-exchange protocol.

17. The node of claim 16, wherein

the key-exchange protocol corresponds to a Needham-Schroeder key-exchange protocol.

18. The node of claim 15, wherein

the query and response correspond to at least a portion of an OCPS protocol initiated by the node.

19. The node of claim 15, wherein

the measure of processing time is predefined.

20. The node of claim 15, wherein

the processor is configured to determine the proximity based on a comparison of the communication time to a threshold value that distinguishes between local and remote nodes.

21. The node of claim 15, wherein

the processor is further configured to control subsequent communications with the target node based on the proximity.

1/1

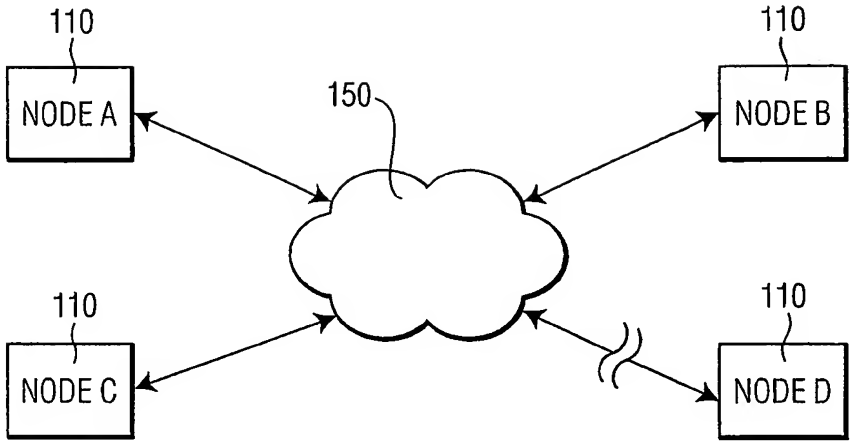

110
NODE A
150
110
NODE B
110
NODE C
110
NODE D

FIG. 1

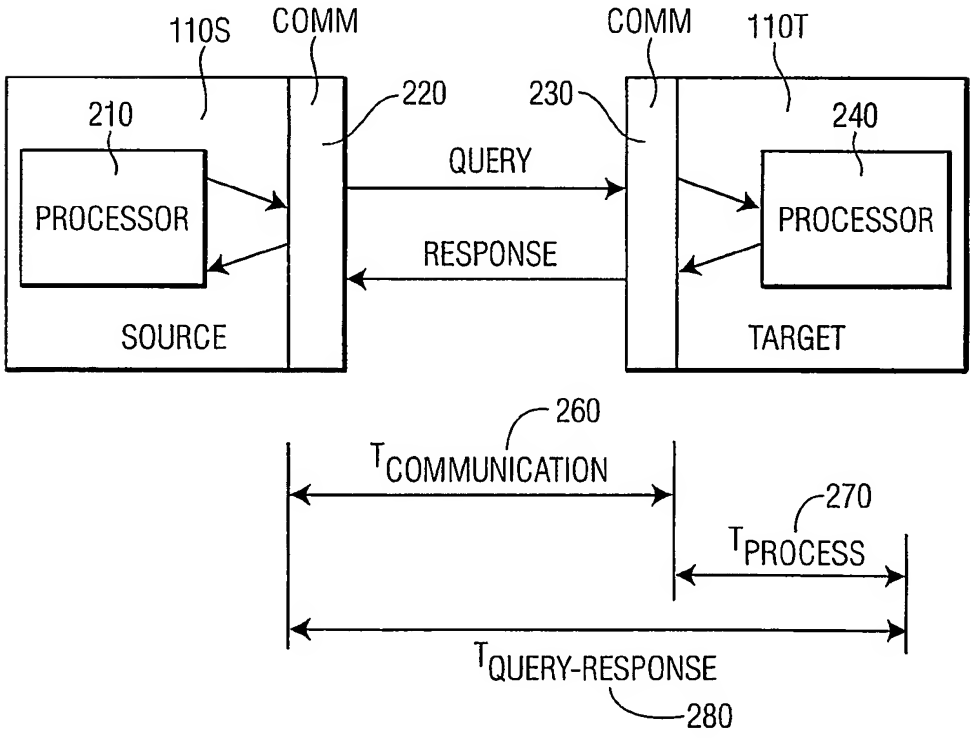

110S
COMM
COMM
110T
220
230
210
240
QUERY
PROCESSOR
PROCESSOR
RESPONSE
SOURCE
TARGET
260
TCOMMUNICATION
270
TPROCESS
TQUERY-RESPONSE
280

FIG. 2

INTERNATIONAL SEARCH REPORT

International Appli o
PCT/IB [redacted]04123

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	STEVENS ET AL: "TCP/IP ILLUSTRATED, Vol. 1. THE PROTOCOLS" TCP/IP ILLUSTRATED. VOL. 1: THE PROTOCOLS, PROFESSIONAL COMPUTING SERIES, READING, MA: ADDISON WESLEY, US, vol. 1, 1994, pages 85-96, XP002106390 ISBN: 0-201-63346-9	1,9,15
A	page 85 -page 87	2-8, 10-14, 16-21

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 January 2004	03/02/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Raposo Pires, J

1

INTERNATIONAL SEARCH REPORT

International Appl[illegible]lo
PCT/IB[illegible]04123

C.(Continuation) DOCUMENTS CONSIDERE[illegible]SE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	NEEDHAM R M ET AL: "Using encryption for authentication in large networks of computers" COMMUNICATIONS OF THE ASSOCIATION FOR COMPUTING MACHINERY, ASSOCIATION FOR COMPUTING MACHINERY. NEW YORK, US, vol. 21, no. 12, December 1978 (1978-12), pages 993-999, XP002163714 ISSN: 0001-0782 the whole document ---	2,3,10, 11,16,17
A	US 6 367 018 B1 (JAIN VIPIN K) 2 April 2002 (2002-04-02) figure 4 column 2, line 52 -column 3, line 22 column 5, line 17 - line 33 ---	1-21
A	FRANCIS P ET AL: "An architecture for a global Internet host distance estimation service" INFOCOM '99. EIGHTEENTH ANNUAL JOINT CONFERENCE OF THE IEEE COMPUTER AND COMMUNICATIONS SOCIETIES. PROCEEDINGS. IEEE NEW YORK, NY, USA 21-25 MARCH 1999, PISCATAWAY, NJ, USA,IEEE, US, 21 March 1999 (1999-03-21), pages 210-217, XP010323734 ISBN: 0-7803-5417-6 page 210 -----	1-21

BEST AVAILABLE COPY

INTERNATIONAL SEARCH REPORT

International Appl lo
PCT/IB [redacted]04123

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6367018 B1	02-04-2002	NONE	

patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.